

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference <b>UCLARF.004VP</b>	<b>FOR FURTHER ACTION</b> see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. <b>PCT/US2005/004877</b>	International filing date (day/month/year) <b>11/02/2005</b>	(Earliest) Priority Date (day/month/year) <b>13/02/2004</b>
Applicant  <b>THE REGENTS OF THE UNIVERSITY OF CALIFORNIA</b>		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 7 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

**1. Basis of the report**

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box II).

3. ☒ **Unity of invention is lacking** (see Box III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☐ the text is approved as submitted by the applicant.

☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 7

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

- b. ☐ none of the figures is to be published with the abstract.

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US2005/004877

## Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-6, 8-12, 23-26

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-6,8-12,23-26

dynamic differential logic, i.e., dual-rail implementations  
with precharge and evaluation phases

---

2. claim: 7

division of a (dynamic differential) logic circuit into two  
separate logic trees

---

3. claims: 13-22

methods for differential pair conductor routing in a logic  
circuit

---

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2005/004877

Box No. IV Text of the abstract (Continuation of item 5 of the first sheet)

DPA-resistant logic circuits and routing are described. An architecture and methodology are suitable for integration in a common automated EDA design tool flow. The architecture and design methodology can be used in logic circuits, gate arrays, FPGAs, cryptographic processors, etc. In one embodiment, the implementation details of how to create a secure encryption module can be hidden from the designer. The designer is thus, able to write the code for the design of DPA-resistant logic circuits using the same design techniques used for conventional logic circuits. Contrary to other complicated DPA-blocking techniques, the designer does not need specialized knowledge and understanding of the methodology. In one embodiment, the automated design flow generates a secure design from a Verilog or VHDL netlist. The resulting encryption module has a relatively constant power consumption that does not depend on the input signals and is thus relatively independent of which logic operations are performed.

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/US2005/004877

## A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F7/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>US 6 329 846 B1 (DAVIES ANDREW DOUGLAS ET AL) 11 December 2001 (2001-12-11)</p> <p>abstract column 1, line 56 - column 2, line 48 figure 5</p> <p>----- -/--</p>	<p>1-6, 8-12, 23-26</p>

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

\* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&amp;" document member of the same patent family

Date of the actual completion of the international search

12 July 2005

Date of mailing of the international search report

10-04-2006

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Post, K

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/US2005/004877

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>RUIZ G A ET AL: "Compact 32-bit CMOS adder in multiple-output DCVS logic for self-timed circuits"</p> <p>IEE PROCEEDINGS: CIRCUITS DEVICES AND SYSTEMS, INSTITUTION OF ELECTRICAL ENGINEERS, STENVENAGE, GB, vol. 147, no. 3, 8 June 2000 (2000-06-08), pages 183-188, XP006013854 ISSN: 1350-2409 abstract page 183, line 31 - line 39 figure 1</p>	1-6, 8-12, 23-26
X	<p>EP 0 921 639 A (HEWLETT-PACKARD COMPANY) 9 June 1999 (1999-06-09)</p> <p>abstract column 6, line 18 - column 7, line 22 figure 6</p>	1-6, 8-12, 23-26
X	<p>US 6 265 923 B1 (AMIR CHAIM ET AL) 24 July 2001 (2001-07-24)</p> <p>abstract column 3, line 39 - line 64 figure 4</p>	1-6, 8-12, 23-26

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US2005/004877

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6329846	B1	11-12-2001	NONE
-----			
EP 0921639	A	09-06-1999	DE 69830968 D1 01-09-2005
			JP 3519959 B2 19-04-2004
			JP 11237447 A 31-08-1999
			US 6075386 A 13-06-2000
-----			
US 6265923	B1	24-07-2001	NONE
-----			